PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-074836

(43)Date of publication of application : 15.03.2002

---

(51)Int.Cl. G11B 20/10
G06F 13/00
H04N 5/85
H04N 5/92
H04N 5/93

---

(21)Application number : 2000-268971 (71)Applicant : CANON INC

(22)Date of filing : 05.09.2000 (72)Inventor : ANDO TSUTOMU

---

(54) MULTIMEDIA DATA RECORDER, OFFICIAL TIME INFORMATION SUPPLYING DEVICE, REPRODUCER, REPRODUCTION SYSTEM, RECORDING METHOD, REPRODUCTION METHOD AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To optionally set a time limit when the contents recorded on a recording medium can be read.

SOLUTION: A multimedia data recorder is provided with a media data enciphering means to encipher the media data by the use of the cipher key information including the time information and a media data recording means which records the media data enciphered by the media data enciphering means on a recording medium. Then it is limited not to reproduce the contents recorded on the recoding medium in the periods

other than the reproduction enabled dates, and it is made possible to distribute the media before the scheduled selling date of the contents or to control the reproduction end date.

LEGAL STATUS [Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The recording device of the multimedia data characterized by providing a media data encryption means by which media data encipher media data including refreshable date information using a cryptographic key, and a media data-logging means to record the media data enciphered by said media data encryption means on a record medium.

[Claim 2] The recording device of the multimedia data characterized by providing a record means by which media data record a refreshable period setting means to set up refreshable date information, a refreshable date information encryption means to encipher the date information to which it was set by said refreshable period setting means using predetermined key information, and said enciphered date information and said media data on a record medium.

[Claim 3] The recording apparatus of the multimedia data characterized by providing a media data coding means to be the recording apparatus of multimedia data according to claim 1 or 2, and to encode said media data accommodative.

[Claim 4] The recording apparatus of the multimedia data characterized by providing a media data encryption means to encipher the media data which are the recording apparatus of multimedia data given in any 1 term of claims 1-3, and were encoded by said media data coding means.

[Claim 5] The official time information feeder characterized by providing an official time information generating means to generate official time information, an official time information encryption means to encipher the current official time information generated by said official time information generating means using the key information prepared beforehand, and an official time-of-day information-transmission means to transmit the current official time information enciphered by said official time information encryption means through a network.

[Claim 6] The regenerative apparatus of the multimedia data characterized by providing an official time information acquisition means to download official time information through a network at the time of the playback check of the enciphered media data including refreshable date information, and a media data playback means to reproduce said media data using the official time information acquired by said official time information acquisition means.

[Claim 7] It is the regenerative apparatus of the multimedia data characterized by being the regenerative apparatus of multimedia data according to claim 6, and said

media data playback means including a decryption-ized means to decode the enciphered media data.

[Claim 8] An information reading means to read the enciphered media data which are recorded on the record medium, A date information extract means to extract the enciphered refreshable date information out of the media data read in the record medium by said information reading means, A time information decryption-ized means to decryption-ize refreshable date information extracted by said date information extract means using predetermined key information, An official time information decryption-ized means to decryption-ize enciphered official time information which is transmitted via a network, A comparison means to compare the refreshable date information read in said record medium with the official time information acquired from said network, The regenerative apparatus of the multimedia data characterized by providing a media data playback means to reproduce the media data read from said record medium, according to the result of a comparison of said comparison means.

[Claim 9] It is the regenerative apparatus of the multimedia data characterized by being the regenerative apparatus of multimedia data according to claim 8, and said media data playback means including a decryption-ized means to decode the enciphered media data.

[Claim 10] An official time information generating means to be the regeneration system of the multimedia data which consist of an official time information feeder and a regenerative apparatus of multimedia data, and to generate official time information, An official time information encryption means to encipher the official time information generated by said official time information generating means using the key information prepared beforehand, Said official time information feeder is equipped with an official time-of-day information-transmission means to transmit the official time information enciphered by said official time information encryption means through a network. An official time information acquisition means to download official time information through said network when reproducing the media data including refreshable date information enciphered from a record medium, The media data read from said record medium The regeneration system of the multimedia data characterized by equipping the regenerative apparatus of said multimedia data with a media data playback means to reproduce based on the official time information acquired by said official time information acquisition means, and said refreshable date information.

[Claim 11] The record approach of the multimedia data characterized by performing media data encryption processing in which media data encipher media data including refreshable date information using a cryptographic key, and media data-logging

processing which records the media data enciphered by said media data encryption processing on a record medium.

[Claim 12] The record approach of the multimedia data characterized by to perform the record processing which records refreshable period setting processing of setting up the date information in which media data include refreshable time and period, the refreshable date information encryption processing which encipher the date information set up by said refreshable period setting processing using predetermined key information, and said enciphered date information and said media data on a record medium.

[Claim 13] The official time information supply approach of carrying out carrying out official time information generating processing in which official time information is generated, the official time information encryption processing which enciphers the official time information generated by said official time information generating processing using the key information prepared beforehand, and official time-of-day information-transmission processing in which the official time information enciphered by said official time information encryption processing is transmitted through a network as the description.

[Claim 14] The playback approach of the multimedia data characterized by performing official time information acquisition processing which downloads official time information through a network at the time of the playback check of the enciphered media data including refreshable date information, and media data regeneration which reproduces said media data using the official time information acquired by said official time information acquisition processing.

[Claim 15] Information reading processing in which the enciphered media data which are recorded on the record medium are read, Date information extract processing in which the enciphered refreshable date information is extracted out of the media data read in the record medium by said information reading processing, The date information decryption-ized processing which decryption-izes refreshable date information extracted by said date information extract processing using predetermined key information, The official time information decryption-ized processing which decryption-izes enciphered official time information which is transmitted via a network, The comparison processing which compares the refreshable date information read in said record medium with the official time information acquired from said network, The playback approach of the multimedia data characterized by performing media data regeneration which reproduces the media data read from said record medium according to the result of a comparison of said

comparison processing.

[Claim 16] Official time information generating processing in which are the playback approach of the multimedia data using an official time information feeder and the regenerative apparatus of multimedia data, and official time information is generated, The official time information encryption processing which enciphers the official time information generated by said official time information generating processing using the key information prepared beforehand, Said official time information feeder performs official time-of-day information-transmission processing in which the official time information enciphered by said official time information encryption processing is transmitted through a network. The official time information acquisition processing which downloads official time information through said network when reproducing the media data including refreshable date information enciphered from a record medium, The media data read from said record medium The playback approach of the multimedia data characterized by the regenerative apparatus of said multimedia data performing media data regeneration reproduced based on the official time information acquired by said official time information acquisition processing and said refreshable date information.

[Claim 17] The storage characterized by storing in any 1 term of claims 11-16 from a computer the program which performs the approach of a publication possible [read-out].

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention is used in order to restrict the refreshable date of multimedia contents recorded on the record medium about the recording device, the official time information feeder, the regenerative apparatus, the regeneration system, the record approach, the playback approach, and storage of multimedia data, and it is suitable.

[0002]

[Description of the Prior Art] Distribution and the various approaches of transmitting are devised from the former, managing the copyright and the playback conditions of multimedia data. The example is shown below.

[0003] Drawing 6 is the example of DVD (digital video disc). Setting to drawing 6 , 601 is MPU (Micro Processing Unit: IC which accumulated the function of the central processing unit of a computer on one chip.). it is also called a microprocessor. it is —— the whole control is managed.

[0004] 602 is security management equipment, and only when playback conditions are ready for every Media, it outputs the decode key for carrying out decoding of the code. 603 is equipment which plays decoded video (or an audio playback), and the loudspeaker which accompanies a monitoring device and it hits this. Moreover, 604 is a bus which performs the whole data transmission.

[0005] 605 is a DVD drive and is equipment which carries DVD media. 606 is decryption-ized equipment and does the decryption-ized activity of media using the cryptographic key which security management equipment 602 outputs. 608 is a DVD disk. This DVD disk itself can be enciphered by the specific encryption technique, when managing copyright.

[0006] In the case of the DVD disk 608, the function in which a region code restricts whether it is refreshable according to the area of each country is prepared. Said regional codes (regional code) are the disk of DVD-Video specification, and the area number attached to the drive which reproduces this. In the combination whose number of this does not correspond, a disk is unreproducible. The whole world is divided into six areas, it is specified, and the regional code which a manufacturer means can be recorded on a disk. Not only one but the thing for which more than one are recorded is possible for a regional code.

[0007] The decryption-ized media data are sent to the media decoder 607. In the case of DVD, a video data is MPEG-2, audio data have been the specification encoded by AC3, but especially an encoding method is not explained. In the media decoder 607,

video audio data are divided into each (demultiplexing), and it is decoded by each decoder (decode).

[0008]

[Problem(s) to be Solved by the Invention] Since the time which reproduces the contents recorded on the record medium was not able to be restricted according to the Prior art, it was possible to have reproduced, just as it provides a user with said record medium.

[0009] For this reason, since the scheduled day could not be made to peruse contents all at once when the record medium was distributed to each user before the scheduled day which puts contents on the market, the problem which must distribute a record medium to a user intensively was in the sale day.

[0010] Moreover, since change did not arise in playback quality even if long time amount passed, the user could use forever the contents distributed gratuitously, and the contents recorded on the conventional record medium had a problem with it difficult [to sell charged contents], when contents were distributed gratuitously.

[0011] This invention aims at enabling it to set as arbitration the term which can peruse the contents recorded on the record medium in view of the above-mentioned trouble.

[0012]

[Means for Solving the Problem] The recording apparatus of the multimedia data of this invention is characterized by providing a media data encryption means by which media data encipher media data including refreshable date information using a cryptographic key, and a media data-logging means to record the media data enciphered by said media data encryption means on a record medium. Moreover, it is characterized by for the recording apparatus of the multimedia data of this invention to possess a record means by which media data record a refreshable period setting means to set up refreshable date information, a refreshable date information encryption means to encipher the date information to which it was set by said refreshable period setting means using predetermined key information, and said enciphered date information and said media data on a record medium. Moreover, the official time information feeder of this invention is characterized by providing an official time information generating means to generate official time information, an official time information encryption means to encipher the current official time information generated by said official time information generating means using the key information prepared beforehand, and an official time-of-day information-transmission means to transmit the current official time information

enciphered by said official time information encryption means through a network. Moreover, the regenerative apparatus of the multimedia data of this invention is characterized by providing an official time information acquisition means to download official time information through a network at the time of the playback check of the enciphered media data including refreshable date information, and a media data playback means to reproduce said media data using the official time information acquired by said official time information acquisition means. Moreover, the regenerative apparatus of the multimedia data of this invention An information reading means to read the enciphered media data which are recorded on the record medium, A date information extract means to extract the enciphered refreshable date information out of the media data read in the record medium by said information reading means, A time information decryption-ized means to decryption-ize refreshable date information extracted by said date information extract means using predetermined key information, An official time information decryption-ized means to decryption-ize enciphered official time information which is transmitted via a network, A comparison means to compare the refreshable date information read in said record medium with the official time information acquired from said network, It is characterized by providing a media data playback means to reproduce the media data read from said record medium, according to the result of a comparison of said comparison means. Moreover, the regeneration system of the multimedia data of this invention An official time information generating means to be the regeneration system of the multimedia data which consist of an official time information feeder and a regenerative apparatus of multimedia data, and to generate official time information, An official time information encryption means to encipher the official time information generated by said official time information generating means using the key information prepared beforehand, Said official time information feeder is equipped with an official time-of-day information-transmission means to transmit the official time information enciphered by said official time information encryption means through a network. An official time information acquisition means to download official time information through said network when reproducing the media data including refreshable date information enciphered from a record medium, It is characterized by equipping the regenerative apparatus of said multimedia data with a media data playback means to reproduce the media data read from said record medium based on the official time information acquired by said official time information acquisition means, and said refreshable date information. Moreover, the record approach of the multimedia data of this invention is characterized by performing media data encryption processing in

which media data encipher media data including refreshable date information using a cryptographic key, and media data-logging processing which records the media data enciphered by said media data encryption processing on a record medium. Moreover, the record approach of the multimedia data of this invention is characterized by to perform the record processing which records refreshable period setting processing of setting up the date information in which media data include refreshable time and period, the refreshable date information encryption processing which encipher the date information set up by said refreshable period setting processing using predetermined key information, and said enciphered date information and said media data on a record medium. Moreover, the official time information supply approach of this invention carries out carrying out official time information generating processing in which official time information is generated, the official time information encryption processing which enciphers the official time information generated by said official time information generating processing using the key information prepared beforehand, and official time-of-day information-transmission processing in which the official time information enciphered by said official time information encryption processing is transmitted through a network as the description. Moreover, the playback approach of the multimedia data of this invention is OFISHA acquired by the official time information acquisition processing which downloads official time information through a network at the time of the playback check of the enciphered media data including refreshable date information, and said official time information acquisition processing. It is characterized by performing media data regeneration which reproduces said media data using RU time information. Moreover, the playback approach of the multimedia data of this invention Information reading processing in which the enciphered media data which are recorded on the record medium are read, Date information extract processing in which the enciphered refreshable date information is extracted out of the media data read in the record medium by said information reading processing, The date information decryption-ized processing which decryption-izes refreshable date information extracted by said date information extract processing using predetermined key information, The official time information decryption-ized processing which decryption-izes enciphered official time information which is transmitted via a network, The comparison processing which compares the refreshable date information read in said record medium with the official time information acquired from said network, It is characterized by performing media data regeneration which reproduces the media data read from said record medium according to the result of a comparison of said comparison processing. Moreover, the

playback approach of the multimedia data of this invention Official time information generating processing in which are the playback approach of the multimedia data using an official time information feeder and the regenerative apparatus of multimedia data, and official time information is generated, The official time information encryption processing which enciphers the official time information generated by said official time information generating processing using the key information prepared beforehand, Said official time information feeder performs official time-of-day information-transmission processing in which the official time information enciphered by said official time information encryption processing is transmitted through a network. The official time information acquisition processing which downloads official time information through said network when reproducing the media data including refreshable date information enciphered from a record medium, It is characterized by the regenerative apparatus of said multimedia data performing media data regeneration which reproduces the media data read from said record medium based on the official time information acquired by said official time information acquisition processing and said refreshable date information. Moreover, the place by which it is characterized [of the storage of this invention] is characterized by storing from a computer the program which performs an approach given in above any they are possible [read-out].

[0013]

[Embodiment of the Invention] The gestalt of operation of the 1st of the recording device of the multimedia data of this invention, an official time information feeder, a regenerative apparatus, a regeneration system, the record approach, the playback approach, and a storage is explained below <the gestalt of the 1st operation>, referring to an accompanying drawing. Drawing 1 is the block diagram showing an example of the regeneration system of the multimedia data of the gestalt of this operation.

[0014] In drawing 1 , 101 is the record medium of media data. With the gestalt of this operation, it does not limit especially about the class of record medium, and if it is the media which can sufficiently follow in footsteps of the rate which reads each media data, various record media can be used.

[0015] 102 is a media reader. The media data read with this media reader 102 shall be enciphered so that it may mention later, referring to drawing 2 .

[0016] 103 is a time information extractor and extracts only time information from the read media data. Although said time information shows refreshable time information, this information shall be enciphered beforehand. 105 is a time information decoder and

time information is decoded with the master key outputted by the master key generator 104.

[0017] An example of said time information is shown in drawing 4 . In drawing 4 , 401-406 show initiation time information. respectively -- 401 -- in an opening day and 404, at the time of initiation, 405 shows a started part and, as for an initiation year and 402, 406 shows [the initiation moon and 403] the initiation second.

[0018] On the other hand, 407-412 are the same and termination time information is shown. 413 is option data and adds the data of arbitration, such as data for an error collection, contents tbe data (truck data), and a sum check.

[0019] 407 [moreover,] -- in an end date and 410, at the time of termination, 411 shows an ended part and, as for a termination year and 408, 412 shows [the termination moon and 409] the termination second. Anyway, said data stream is enciphered using a master key.

[0020] It is equipment which compares with drawing 1 the official time information transmitted from the network which return and 107 are time comparators and is mentioned later. When it was refreshable time and is checked as a comparison result of the time comparator 107, decryption is performed by the media decryptor 106, and by the media regenerator 108, media playback is performed and it is displayed on a display 110.

[0021] The authorized time information which is sent from a server side is sent through a network 112, and is received by network connection equipment 111. And said authorized time information is decoded by the time information decoder 109, and is given to the time comparator 107.

[0022] 113-116 are each function which constitutes an official time-of-day generating server. 113 is a time information generator and generates exact time of day. 114 is a time information code machine and enciphers time information with the master key generated by the master key generator 116. 115 is network connection equipment and transmits the enciphered time information to a client.

[0023] The flow chart of the transceiver procedure of data performed to drawing 2 between server clients is shown. If processing is started as shown in drawing 2 , in the first step S201, the data reproduced from media by the client side will be read, and it will check whether the data is enciphered (step S203).

[0024] As a result of the check of step S203, when not enciphered, it reproduces as it is (step S202). At step S202, the data reproduced from media will decrypt, if compression coding of MPEG-2 and the 4 grades is carried out. When enciphered as a result of the check of step S203, while progressing to step S204 and performing the

Request to Send of an official time to a server, the refreshable time-of-day data enciphered from media are extracted (step S205).

[0025] On the other hand, in a server side, official time information is acquired according to the demand from a client (step S214). Next, a master key is acquired (step S217), official time information is enciphered using this master key (step S215), and this is transmitted to a client (step S216).

[0026] An example of official time information is shown in drawing 5 . 507 is option data and he is trying to add the data of arbitration, such as data for an error collection, contents tbe data (truck data), and a sum check, in drawing 5 .

[0027] the official moon and 503 are an official day and, as for 505, an official year and 502 are [501 / 504] moreover, official at the time of official -- a part -- 506 shows the official second.

[0028] It is received by the client side (step S206), and said transmitted official time information which was enciphered is **. Next, a master key is acquired (step S211) and both hour entries are decoded (step S207). Next, both hour entries are compared (step S208).

[0029] Next, it progresses to step S209 and the result of said comparison judges whether it is refreshable time. Specifically, the playback initiation time recorded on media makes playback possible, only when early and playback termination time is later than an official time from an official time.

[0030] As a result of decision of step S209, in not being refreshable time, it progresses to step S210 and ends processing. Moreover, in being in refreshable time as a result of decision of step S209, it decrypts media (step S212). The key information at this time is later mentioned by drawing 3 . When media are made coincidence in compression coding of MPEG-2 and 4 grades, it is decoded suitably and, finally it reproduces (step S213).

[0031] thus, the official time transmitted at any time from a server by constituting -- responding -- the time of arbitration to each contents -- being refreshable (or impossible) -- it becomes possible to carry out.

[0032] In addition, since the reason for downloading time information from a server may be unable to keep the open time for which the provider of contents asks when time of day has been changed by the illegal user if the timer value reserved in the client side is used, it is for preventing this.

[0033] An example of the equipment which enciphers media to drawing 3 is shown. In drawing 3 , 302 is a refreshable time setting device and sets up playback initiation of the contents recorded, and termination time. in addition, initiation and termination --

the case where there is no need of deciding on one of time -- for example, "00 etc. months, 0000" etc. -- as -- what is necessary is just to use it

[0034] 303 is refreshable time encryption equipment and enciphers the time information set up with the refreshable time setting device 302 with the master key outputted from the master key generator 301. 304 is media coding / encryption equipment, and carries out compression coding if needed for each media. Then, it enciphers again by the cryptographic key outputted from refreshable time encryption equipment 303. 305 is a media recording apparatus and is for writing in an archive medium 306.

[0035] In the example shown in drawing 1 carried out, the master key was the premise that the common key was beforehand saved to a client and each server by a certain approach, the <gestalt of the 2nd operation> above-mentioned. This can also be serially transmitted by the secure session between server clients. Moreover, it is also possible to carry in a device like ROM (Read Only memory) beforehand in a regenerative apparatus. In addition, in this example, although explained using the common key system, the configuration which takes the cipher system using a public key system between server clients is also possible. Moreover, it is also possible by adopting a hierarchical key method to build a method with more high security as the key finally used for encryption is adopted with DVD.

[0036] Moreover, all this inventions can also be mounted by software. moreover, the time of permitting playback -- separately -- an accounting system -- contents -- receiving -- accounting -- a line -- things are also possible.

[0037] Moreover, of course, it is also possible to also perform a date limit uniformly to two or more contents recorded on media and to specify for every internal truck or file, although it is possible.

[0038] (Gestalt of other operations of this invention) Even if it applies this invention to the system which consists of two or more devices (for example, a host computer, an interface device, a reader, a printer, etc.), it may be applied to the equipment which consists of one device.

[0039] Moreover, so that the function of the gestalt of operation mentioned above may be realized and various kinds of devices may be operated As opposed to the computer in the equipment connected with said various devices, or a system The program code of the software for realizing the function of the gestalt of said operation is supplied. What was carried out by operating said various devices according to the program stored in the computer (CPU or MPU) of the system or equipment is contained under the category of this invention.

[0040] Moreover, the function of the gestalt of operation which the program code of said software itself mentioned above in this case will be realized, and the storage which stored the means for supplying that program code itself and its program code to a computer, for example, this program code, constitutes this invention. As a storage which memorizes this program code, a floppy (trademark) disk, a hard disk, an optical disk, a magneto-optic disk, CD-ROM, a magnetic tape, the memory card of a non-volatile, ROM, etc. can be used, for example.

[0041] Moreover, by performing the program code with which the computer was supplied, also when functions jointly shown with the gestalt of the above-mentioned operation, such as OS (operating system) or other application software with which an explanation function is not only realized, but the program code is working in a computer with the gestalt of the above-mentioned operation, are realized, it cannot be overemphasized that this program code is contained in the gestalt of operation of this invention.

[0042] Furthermore, after stored in the memory with which the functional expansion unit by which the supplied program code was connected to the functional add-in board and the computer of a computer is equipped, a part or all of processing that CPU with which the functional add-in board and functional expansion unit are equipped based on directions of the program code is actual performs, and it is contained in this invention also when the function of the gestalt of operation mentioned above by the processing is realized.

[0043]

[Effect of the Invention] Since according to this invention this invention sets up a playback date limit and recorded contents on the record medium as mentioned above, it can restrict at stages other than said set-up refreshable date so that the contents currently recorded on said record medium may not be reproduced. This becomes possible to distribute a record medium to a user before the scheduled day which puts contents on the market, and the problem which circulates a record medium intensively on a sale day can be avoided. Moreover, since much contents can be recorded on the record medium of one sheet and a refreshable date can be set up for every contents, contents can be made refreshable one by one in the time in alignment with a distribution person's intention, and even if it distributes the record medium beforehand, day by day [predetermined] can be provided with contents. Moreover, expansion of the business it invites from the contents distributed gratuitously to charged contents can be enabled by controlling playback quality according to time amount progress.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the gestalt of 1 operation of this invention.

[Drawing 2] It is a flow chart explaining the operations sequence of the gestalt of the 1st operation.

[Drawing 3] It is the block diagram showing the example of a configuration of a media recording apparatus.

[Drawing 4] It is drawing showing an example of playback initiation / termination time data.

[Drawing 5] It is drawing showing an example of official time-of-day data.

[Drawing 6] It is the block diagram showing the conventional example.

[Description of Notations]

101 Record Medium of Media Data

102 Media Reader

103 Time Information Extractor

104 Master Key Generator

105 Time Information Decoder

106 Media Decryptor

107 Time Comparator

108 Media Regenerator

109 Time Information Decoder

110 Display
111 Network Connection Equipment
112 Network
113 Time Information Generator
114 Time Information Code Machine
115 Network Connection Equipment
116 Master Key Generator